27. Связь задачи разложения правильной дроби в сумму простейших с интерполяцией. Критерий отсутствия кратных корней.

Мини напоминание что такое простейшая дробь.

Определение

Дробь $\frac{f}{g} \in K(t)$ — **простейшая**, если $g = p^k$, где $p \in K[t]$ — неприводимый многочлен и $\deg(f) < \deg(p)$.

- Пусть K — поле. Покажем простой способ разложения на простейшие правильной дроби $\frac{f(x)}{g(x)} \in K(x)$, где $g(x) = (x - a_1)\dots(x - a_n)$, и $a_1, \dots, a_n$ различны.
- Рассмотрим интерполяционную задачу с точками a_1, $\dots$, a_n и значениями $f(a_1)$, $\dots$, $f(a_n)$ в них соответственно.
- Так как $\deg(f) < n$, многочлен f и есть единственный интерполяционный многочлен для рассматриваемой задачи. Запишем формулу Лагранжа:

$$f(x) = \sum_{i=1}^{n} \frac{f(a_i)}{g'(a_i)} \frac{g(x)}{x - a_i} \quad \Rightarrow \quad \frac{f(x)}{g(x)} = \sum_{i=1}^{n} \frac{f(a_i)}{g'(a_i)} \frac{1}{x - a_i}.$$

- Мы получили разложение $\frac{f(x)}{g(x)}$ на простейшие.

Рассмотрим пример.

$f(x) = x^2 + 3$

$g(x) = (x - 3)(x - 4)(x - 5) = x^3 - 12x^2 + 47x - 60$

$g'(x) = 3x^2 - 24x + 47$

$$\frac{f(x)}{g(x)} = \frac{f(3)}{g'(3)}\frac{1}{x-3} + \frac{f(4)}{g'(4)}\frac{1}{x-4} + \frac{f(5)}{g'(5)}\frac{1}{x-5} =$$

$$= \frac{6}{x-3} + \frac{-19}{x-4} + \frac{14}{x-5} = \frac{x^2+3}{x^3 - 12x^2 + 47x - 60}$$

• А как понять, что многочлен не имеет кратных корней?

Лемма 12

1) *Если K — поле и многочлен $g \in K[t]$ таков $(g, g') \sim 1$, то g не имеет кратных корней (то есть, корней кратности более 1).*

2) *Если многочлен $g \in \mathbb{C}[t]$ не имеет кратных корней, то $(g, g') \sim 1$.*

Доказательство. 1) Если g имеет корень α кратности не менее 2, то α — корень g' по Теореме 8. Тогда $(g, g') \vdots (t - \alpha)$, противоречие.

> Теорема 8
> *Пусть K — поле, $\mathrm{char}(K) = 0$, $f \in K[t]$, $\alpha \in K$ — корень f. Тогда α — корень кратности m многочлена f, если и только если $f(\alpha) = 0$, $f'(\alpha) = 0$, $\dots$, $f^{(m-1)}(\alpha) = 0$, а $f^{(m)}(\alpha) \neq 0$.*

2) • Так как g не имеет кратных корней, по Теореме 8 ни один из корней g не является корнем g'.

• Если при этом $(g, g') \sim h$, $\deg(h) \geq 1$, то h по основной теореме алгебры, имеет корень, который является общим корнем g и g', противоречие. $\square$

> Теорема 9
> *Любой многочлен из $\mathbb{C}[t]$ имеет корень из $\mathbb{C}$.*

28. Поле C, как факторкольцо R[x].
Впереди самые жуткие штуки. Напомним что такое фактор кольцо.

Факторкольцо

- Для $a \in K$ вычет, состоящий из элементов кольца, сравнимых с a, как правило, будем обозначать через $\bar{a}$.
- Из определения следует, что $\bar{a} = a + I = \{a + x \; : \; x \in I\}$.

Определение

- Пусть K — коммутативное кольцо, I — идеал в K.

Факторкольцо $K/I := \{\bar{a} \; : \; a \in K\}$.

- $\bar{a} + \bar{b} := \overline{a+b}; \qquad \bar{a} \cdot \bar{b} := \overline{ab}.$

Теорема 14

$$\mathbb{C} \simeq \mathbb{R}[t]/(t^2+1)\mathbb{R}[t].$$

Нам нужно доказать, что фактор-кольцо кольца многочленов над полем R по идеалу многочленов, делящихся на t^2 + 1, изоморфно полю комплексных чисел.

Доказательство. • Определим отображение $\varphi : \mathbb{R}[t] \to \mathbb{C}$ формулой $\varphi(f) := f(i)$.

- Докажем, что φ — гомоморфизм. Пусть $f, g \in K[t]$.
- $\varphi(f+g) = (f+g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g)$;
- $\varphi(fg) = (fg)(i) = f(i) \cdot g(i) = \varphi(f) \cdot \varphi(g)$.
- Докажем, что φ — сюръекция. Пусть $z = a + bi \in \mathbb{C}$, где $a, b \in \mathbb{R}$. Тогда $bt + a \in \mathbb{R}[t]$ и $\varphi(bt+a) = a + bi$.
- Пусть $f \in \mathrm{Ker}(\varphi)$, разделим f с остатком на t^2+1: $f(t) = (t^2+1)g(t) + bt + a$ (степень остатка по определению не превосходит 1, значит, он представляется в виде $bt + a$).
- Тогда $0 = \varphi(f) = f(i) = (i^2+1)g(i) + bi + a = bi + a \iff a = b = 0 \iff f \,\vdots\, t^2 + 1$.
- Таким образом, $\mathrm{Im}(\varphi) = \mathbb{C}$, $\mathrm{Ker}(\varphi) = (t^2+1)\mathbb{R}[t]$ и по теореме о гомоморфизме колец имеем $\mathbb{C} = \mathrm{Im}(\varphi) \simeq \mathbb{R}[t]/\mathrm{Ker}(\varphi) = \mathbb{R}[t]/(t^2+1)\mathbb{R}[t]$. $\square$

Во время поисков в интернете я нашла это:
Два многочлена лежат в одном классе эквивалентности тогда и только тогда, когда они имеют одинаковые остатки при делении на $x^2 + 1$, поэтому фактор-

кольцо можно представить как множество многочленов вида ax+b со стандартным сложением и умножением по правилу: $(ax+b)(cx+d)=(ad+bc)x+(bd-ac)$.

Точно так же перемножаются соответствующие комплексные числа: $(b+ai)(d+ci)=(bd-ac)+(ad+bc)i$.

Поэтому изоморфизм устанавливается правилом: $ax+b \to b+ai$

На мой взгляд это неконструктивное доказательство, но оно помогает понять что мы вообще хотим (закрыть сессию).

29. Многочлен деления круга. Представление $t^n - 1$ в виде произведение многочленов деления круга

Ух, ну что ж поехали.

Немного вспомним:

Определение

Пусть $n \in \mathbb{N}$. Число $\varepsilon \in \mathbb{C}$ такое, что $\varepsilon^n = 1$, но $\varepsilon^k \neq 1$ при натуральных $k < n$ называется *первообразным корнем из 1* степени n.

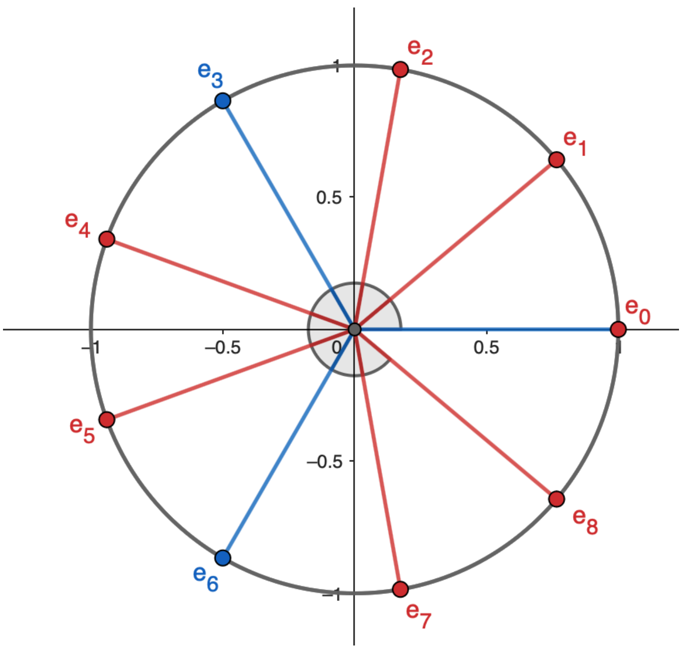
- По Теореме 2.25 существует ровно $\varphi(n)$ первообразных корней из 1 степени n, и они имеют вид $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$, где $k \in \{1, \ldots, n-1\}$, $(k, n) = 1$.

Определение

Многочлен деления круга $\Phi_n(t) := \prod\limits_{1 \le k \le n,\ (k,n)=1} (t - \varepsilon_k)$.

То есть как он выглядит: пусть n = 9

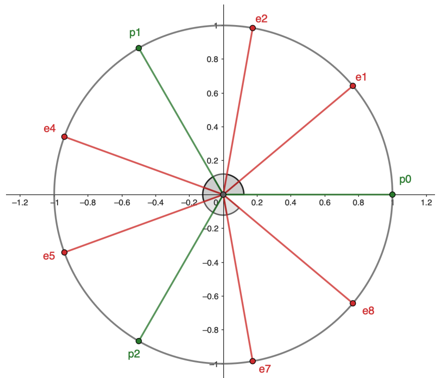
$\Phi_9(t) = (t - \epsilon_1) \cdot (t - \epsilon_2) \cdot (t - \epsilon_4) \cdot (t - \epsilon_5) \cdot (t - \epsilon_7) \cdot (t - \epsilon_8) = t^6 + t^3 + 1$



- Из определения следует, что $\Phi_n \in \mathbb{C}[t]$. Мы докажем, что все коэффициенты этого многочлена целые.

Лемма 13

$t^n - 1 = \prod\limits_{d \mid n} \Phi_d(t).$



Т.е. на нашем примере:

$t^9 - 1 = \Phi_1(t) \cdot \Phi_3(t) \cdot \Phi_9(t) =$

$= [(t - \epsilon_0)] \cdot [(t - \rho_1) \cdot (t - \rho_2)] \cdot [(t - \epsilon_1) \cdot (t - \epsilon_2) \cdot (t - \epsilon_4) \cdot (t - \epsilon_5) \cdot (t - \epsilon_7) \cdot (t - \epsilon_8)] =$

$= (t - 1) \cdot (t^2 + t + 1) \cdot (t^6 + t^3 + 1) = t^9 - 1$

Доказательство. • Если $d \mid n$, то первообразный корень из 1 степени d, очевидно, является корнем из 1 степени n.

Они помечены зеленом на кружочке

• Следовательно, $t^n - 1 \,\vdots\, \Phi_d(t)$.

• Так как каждый корень из 1 является первообразным корнем ровно одной степени, $t^n - 1 \,\vdots\, \prod\limits_{d \mid n} \Phi_d(t)$.

• Пусть $\varepsilon_0, \ldots, \varepsilon_{n-1}$ — все корни степени n из 1, $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$.

• Пусть $(k, n) = d$, $k = k'd$, $n = n'd$. Тогда $\varepsilon_k = (\cos(\frac{2\pi k'}{n'}), \sin(\frac{2\pi k'}{n'}))$.

Теорема 25

1) *Существует в точности $\varphi(n)$ первообразных корней степени n из 1, это в точности такие корни ε_j, что $(j, n) = 1$.*

2) *Если ε_j — первообразный корень степени n из 1, то ε_j, ε_j^2, $\ldots$, ε_j^n — все корни степени n из 1.*

• Так как дробь $(k', n') = 1$, по Теореме 2.25 ε_k — первообразный корень степени n' из 1, причем $n' \mid n$.'

• Следовательно, все корни из 1 степени n являются первообразными корнями степеней-делителей n.

• Следовательно, $t^n - 1 \mid \prod\limits_{d \mid n} \Phi_d(t)$. $\square$

30. Многочлен деления круга: формула, целые коэффициенты.

Теорема 15

1) $$\Phi_n(t) = \prod_{d\,|\,n} (t^d - 1)^{\mu(\frac{n}{d})}. \qquad (*)$$

2) $\Phi_n \in \mathbb{Z}[t]$ — унитарный многочлен (то есть, старший коэффициент Φ_n равен 1).

Например,

$$\Phi_{12}(x) = \left(x^{12}-1\right)\left(x^6-1\right)^{-1}\left(x^4-1\right)^{-1}\left(x^3-1\right)^0\left(x^2-1\right)\left(x-1\right)^0$$
$$= \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1.$$

например

Функция Мёбиуса $\mu(n) :=$
$$\begin{cases} 1, & \text{если } n = 1,\\ (-1)^k, & \text{если } n = p_1 \dots p_k \text{ — произведение различных простых чисел,}\\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Теорема 22

Пусть K — поле, $f, g : \mathbb{N} \to K \setminus \{0\}$, причем $f(m) = \prod_{d\,|\,m} g(d)$.

Тогда $g(m) = \prod_{n\,|\,m} f(n)^{\mu(\frac{m}{n})}$.

Доказательство. 1) • По Лемме 13 имеем $t^n - 1 = \prod_{d\,|\,n} \Phi_d(t)$.

• Теперь $(*)$ непосредственно следует из мультипликативной формулы обращения Мёбиуса (Теоремы 2.22).

$$t^n - 1 = \prod_{d|n} \Phi_d(t) \Rightarrow \Phi_n(t) = \prod_{d|n} (t^d - 1)^{\mu(\frac{n}{d})}$$

2) • Формулу $(*)$ можно переписать в виде $\Phi_n(t) = \frac{f(t)}{g(t)}$, где $f, g \in \mathbb{Z}[t]$ — унитарные многочлены (каждый из f и g представляется в виде произведения нескольких многочленов вида $x^d - 1$).

• При делении в столбик унитарного многочлена f с целыми коэффициентами на унитарный многочлен g с целыми коэффициентами нетрудно убедиться, что неполное частное будет унитарным многочленом с целыми коэффициентами.

• При этом, f разделится на g без остатка и частное получится равным $\Phi_n(t)$. $\square$

А теперь пара интересных штучек. Во-первых, дети в советском союзе это правда проходили в школе. Доказательства.

10 класс — **Многочлены деления круга** — 5 марта 2015

Напоминание. У многочлена $z^n - 1$ есть n различных комплексных корней, а именно числа вида $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ для $k = 0, 1, \ldots, n-1$, которые называются *корнями из единицы n-й степени*. Соответствующие точки на комплексной плоскости располагаются на единичной окружности с центром в нуле и образуют правильный n-угольник. ξ – корень из единицы n-й степени называется *примитивным*, если $\xi^m \neq 1$ для всех натуральных m, меньших n.

1. а) Пусть ξ – корень из единицы n-й степени, $\xi \neq 1$. Найдите сумму $1 + \xi + \xi^2 + \ldots + \xi^{n-1}$.

б) Чему равна сумма всех корней n-й степени из 1? А произведение?

в) А сколько всего примитивных корней из единицы n-й степени?

г) Радиус окружности, описанной около правильного n-угольника, равен 1. Найдите произведение расстояний от его фиксированной вершины A до всех остальных вершин этого многоугольника.

Критерий Эйзенштейна. Пусть все коэффициенты многочлена над $\mathbb{Z}$ (т.е. многочлена с целыми коэффициентами), кроме старшего, делятся на простое число p, и свободный член не делится на p^2. Тогда этот многочлен неприводим над $\mathbb{Z}$ (т.е. не представляется в виде произведения двух непостоянных многочленов с целыми коэффициентами).

2. Докажите, что для любого простого p многочлен $x^{p-1}+x^{p-2}+\ldots+x+1$ неприводим над $\mathbb{Z}$ (подсказка: попробуйте сдвинуть аргумент на 1).

Определение. *Многочлен деления круга* — это $\Phi_n(x) = (x-\xi_1)(x-\xi_2)\ldots(x-\xi_{\varphi(n)})$, где $\xi_1, \xi_2, \ldots \xi_{\varphi(n)}$ – все примитивные корни n-й степени из 1.

3. а) Докажите, что $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

На Московской олимпиаде 1997 года девятиклассники решали задачу, вошедшую в «Задачник «Кванта»:

М1598. *Пусть $1 + x + x^2 + \ldots + x^{n-1} = F(x)G(x)$, $n > 1$, $F(x)$ и $G(x)$ — многочлены с неотрицательными коэффициентами.*

а) Докажите, что все коэффициенты этих многочленов — нули и единицы.

б) Докажите, что один из многочленов $F(x)$, $G(x)$ представим в виде $(1 + x + \ldots + x^{k-1})T(x)$, где $k > 1$, а коэффициенты полинома $T(x)$ — нули и единицы.

Точнее говоря, на олимпиаде было предложено решить пункт б) для многочленов F и G, коэффициенты которых суть нули и единицы. Решил задачу только один школьник, а большинство из остальных 509 участвовавших в олимпиаде девятиклассников вообще не поняли, о чем речь. Дело в том, что М1598 — лишь частичка теории разложений многочленов $f_n(x) = 1 + x + x^2 + \ldots + x^{n-1}$ на множители. Поэтому она выглядит естественной (и красивой, и не очень трудной!) лишь для того, кто интересовался этими разложениями.

Второе фото из журнала квант и там написан один интересный фактик.

Если начать рекурсивно с Φ_1 и по формуле из леммы 13:

$$t^n - 1 = \prod_{d|n} \Phi_d(t),$$ получим

$\Phi_1 = x - 1,\ \Phi_2 = x + 1,\ \Phi_3 = x^2 + x + 1$ и т.д. При этом давайте рассмотрим формулы сокращенного умножения:

$$x^2 - 1 = (x-1)(x+1)$$
$$x^3 - 1 = (x-1)(x^2+x+1)$$
$$x^4 - 1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$$
$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$$
$$\ldots$$
$$x^n - 1 = (x-1)(x^{n-1}+x^{n-2}+\ldots+x+1)$$

И, о Боги, получается что многочлен деления круга с целыми коэффициентами и формулы сокращенного умножения считай одно и тоже. Вы в шоке? Я да.